94

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,176	06/13/2002	Tomoyuki Asano	SONY JP-180	1654

530 7590 06/18/2007

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
SHAW, YIN CHEN	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/069,176	ASANO ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *34,36,38-48 and 50-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *34, 38-48, and 51-73* is/are rejected.

7)☒ Claim(s) *36 and 50* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the Request for Continued Examination (RCE) dated 03/26/2007.
2. Claims 34, 36, 38-48, 50-73 have been submitted for examination.
3. Claims 34, 36, 38-48, 50-73 are pending.
4. Rejections of Independent claims are provided with detailed citations from the prior arts.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 34, 38-48, 51-65, 68, and 70-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Itkis (U.S. Patent 6,880,081) and further in view of Harada et al. (U.S. Patent 6,687,683), Dondeti et al. (U.S. Patent 6,240,188), and Lotspiech et al. (U.S. Patent 6,118,873).

   a. *Referring to Claims 34 and 44:*

      As per Claim 34, Itkis discloses an information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure **[(Fig. 2)]**, said information processing device comprising:

to store one or more node keys, each node key being unique to one node of the network, and a leaf key, the leaf key being unique to the information processing device **[In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)]**;

to calculate a decryption key be decrypting a key block using at least one of the one or more node keys stored in the storage or the leaf key stored in the storage **[Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key**

distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)];

encrypt the decryption key using the key of the information processing device **[At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). Where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis)]**.

Itkis discloses the hardware component for performing the encryption, decryption, and storage processes **[In a preferred embodiment of the present invention, an improved key distribution system is provided (lines 49-50, Col. 2 from Itkis). Each of the components of FIG. 1 is preferably implemented**

in a combination of software and computer hardware, as is well known in the art, and may include special purpose computer hardware, as is also well known in art, in order to increase efficiency of operation (lines 3-7, Col. 8 and Fig. 1). Individual components, described below, of the security element 120 may be implemented in hardware or in any suitable combination of hardware and software, as is well known in the art (lines 5-8, Col. 11 and Fig. 4)].

However, Itkis does not expressly disclose (1) storage and encryption processor within the processing devices for holding the key information, calculate decryption key, and executing encryption/decryption processing, (2) store the encrypted decryption key in at least one of the storage or on a recording medium and other limitations. However, Harada et al. disclose (1) the LSI component, which contains the encryption and decryption units for deriving key information and performing encryption/decryption processes with keys and the storage unit for holding the relevant key information **[The disk key creation unit 1218 creates a 64-bit disk key including the information on the memory card ID that has been given from the memory card ID obtaining unit 1230. Here, a disk key is key data common to all kinds of memory card that is recording medium. The disk key encryption unit 1220 encrypts the disk**

key that has been created by the disk key creation unit 1218 using one of the plurality of master keys 1219 that have been stored in the disk key encryption unit 1220 in advance. The disk key encryption unit 1220 continues to encrypt the same disk key using a different master key 1219 to create the same number of encryption disk keys as that of the master keys 1219, and outputs the created encryption disk keys to the recording unit 1240 in the memory card writer 1200. The title key creation unit 1221 creates an appropriate 64-bit title key and gives the created title key to the title key encryption unit 1222. Here, the title key indicates key data that can be set for each music content (lines 8-24, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 29-34, Col. 13 and unit 1200 in Fig. 2 and 3 from Harada et al.)], and (2) to store the encrypted decrypting key on a recording medium or in a storage area in said information processing device **[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218,**

and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2 from Harada et al.)]. Dondeti et al. further disclose the leaf key being unique to each of said information processing devices and is unique in relation to a leaf key held by any other node within the hierarchical network of nodes **[Each member 22 is assigned a binary ID and these IDs are used to define key associations for each member 22 (lines 30-31, Col. 3). Members are represented by the leaves of a binary key distribution tree 26. Each member 22 generates a unique secret key 28 for itself and each internal node key is computed as a function of the secret keys of its two children. All secret keys 28 are associated with their blinded versions 30, which are**

computed using a one-way function 32 (lines 48-53, Col. 3). Internal nodes are associated with secret keys (lines 2-3, Col. 4)], and the key used in encrypting the calculated decrypting key is the leaf key **[Wherein, the first member uses the blinded keys received from the key association group and the first secret key to calculate an unblinded key of the first internal node (lines 48-51, Col. 2). All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32 (lines 52-53, Col. 3)]**, and Lotspiech et al. disclose the limitation regarding a key together with a generation number, the generation number representing renewal information for the decryption key **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**, and use the generation number to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key **[a thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys**

"S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)].

Itkis, Harada et al., Dondeti et al., and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al., Dondeti et al., and Lotspiech et al. since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.) and (2) to have a system for providing secure communication between many sends and many members (lines 15-17 from Dondeti et al.), and (3) to encrypt the broadcast programs such that an

unauthorized clone receivers cannot easily decrypt the programs (lines 8-10, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis with Harada et al., Dondeti et al., and Lotspiech et al. to obtain the invention as specified in claim 34.

As per Claim 44, it encompasses some limitations that are similar to those of Claim 34. Therefore, these limitations are rejected with the same rationale applied against Claim 34 above. In addition, Harada et al. disclose store the decryption key together with identification information, the identification information being usable to identify data decrypted using the decryption key **[the memory card ID obtaining unit 1230 obtains the memory card ID that is inherent information from the memory card 1300, and gives the obtained memory card ID to the disk key creation unit 1218. When receiving the recording allowance, the recording unit 1240 records that data that have been output from the disk key encryption unit 1220, the title key encryption unit 1222, and the audio data encryption unit 1223 on the memory card 1300 (line 67, Col. 12 and lines 1-7, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key**

that has been created by the title key creation unit 1221 (lines 29-32, Col. 13 from Harada et al.)].

b. *Referring to Claim 36:*

As per Claim 3, Itkis, Harada et al., and Dondeti et al. the information processing device as claimed in claim 34, wherein the key block includes an encrypted renewal node key, and is further operable to decrypt the encrypted renewal node key to obtain the renewal node key using at least one of the node key stored in the storage or a leaf key belonging to a lower layer of the hierarchical network, and stored in the storage **[(lines 51-53, Col. 1; lines 56-59, Col. 2; lines 56-60, Col. 2; lines 9-10 and 54-58, Col. 3; lines 49-56, Col. 9 from Itkis) and (lines 48-53, Col. 3; lines 2-3, Col. 4 from Dondeti et al.)]**, and to calculate the decryption key using the obtained renewal node key **[(lines 55-59, Col. 1 and lines7-18, Col. 10 from Itkis)]**. In addition, Harada et al. disclose the encryption processor as in claim 34.

c. *Referring to Claims 38 and 52:*

As per Claim 38, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 34, wherein the encryption processor is operable to store the decryption key encrypted using the leaf key unique to the information processing device, **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis) and (lines 48-53, Col. 3; lines 2-3, Col. 4 from Dondeti et al.)]**,

the encrypted decryption key being stored together with identification information, the identification information being unique to the information processing device **[(lines 7-11, Col. 10 from Itkis)]**.

As per Claim 52, the rejection of Claim 48 is incorporated. In addition, Claim 52 encompasses limitations that are similar to those of Claim 38. Therefore, it is rejected with the same rationale applied against Claim 38 above.

d. *Referring to Claims 39 and 53:*

As per Claim 39, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 34, wherein the encryption processing is operable to store the decryption key encrypted using the leaf key unique to the information processing device, the encrypted decryption key being stored together with identification information, the identification information identifying data decrypted using the decryption key **[(line 67, Col. 12 and lines 1-7 and 29-32 Col. 13 from Harada et al.) and (lines 48-53, Col. 3; lines 2-3, Col. 4 from Dondeti et al.)]**.

As per Claim 53, the rejection of Claim 48 is incorporated. In addition, Claim 53 encompasses limitations that are similar to

those of Claim 39. Therefore, it is rejected with the same rationale applied against Claim 39 above.

e. *Referring to Claims 40 and 54:*

As per Claim 40, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 34, wherein the decryption key is usable to decrypt encrypted content data in the information processing device **[(lines 48-50, Col. 1 and lines 7-8, Col. 10 from Itkis)]**.

As per Claim 54, the rejection of Claim 48 is incorporated. In addition, Claim 54 encompasses limitations that are similar to those of Claim 40. Therefore, it is rejected with the same rationale applied against Claim 40 above.

f. *Referring to Claims 41 and 55:*

As per Claim 41, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 34, wherein the decryption key is stored on the recording medium and the decryption key is assigned to the recording medium, the decryption key being usable to decrypt encrypted data stored on the recording medium **[(lines 48-50, Col. 1, and lines 7-8, Col. 10 from Itkis) and (lines 25-34 and 39-43, Col. 13 from Harada et al.); *where the title key is the (media) content key and is located in the recording medium*]**.

As per Claim 55, the rejection of Claim 48 is incorporated. In addition, Claim 55 encompasses limitations that are similar to those of Claim 41. Therefore, it is rejected with the same rationale applied against Claim 41 above.

g. *<u>Referring to Claims 42 and 56:</u>*

As per Claim 42, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 34, wherein the decryption key is held in common by a plurality of the information processing devices, the decryption key being a master key usable to decrypt processing devices **(lines 48-50, Col. 1, lines 7-8, Col. 10, and lines 44-48, Col. 9 from Itkis);** ***where K is always the key used for decrypting the content even it is encrypted by different versions of keys*]**.

As per Claim 56, the rejection of Claim 48 is incorporated. In addition, Claim 56 encompasses limitations that are similar to those of Claim 42. Therefore, it is rejected with the same rationale applied against Claim 42 above.

h. *<u>Referring to Claim 43:</u>*

As per Claim 43, it encompasses some limitations that are similar to those of Claim 34. Therefore, these limitations are rejected with the same rationale applied against Claim 34 above.

Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**; determine whether the decryption key having the generation number is stored in the storage **[a thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)]**. In addition, Harada et al. disclose if so, retrieve the decryption key from the storage for use in decrypting encrypted data without having to decrypt the key block **[Note that the recording unit 1240 records the audio data that has been**

transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2). In a reverse order using the encrypted disk key and title key and to replay music by decrypting the audio data (lines 47-49, Col. 13)]. Itkis, Harada et al., Dondeti et al., and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al., Dondeti et al., and Lotspiech et al. since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.) and (2) to have a system for providing secure communication between many sends and many members (lines 15-17 from Dondeti et al.), and (3) to encrypt the broadcast programs such that an

unauthorized clone receivers cannot easily decrypt the programs (lines 8-10, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis with Harada et al., Dondeti et al., and Lotspiech et al. to obtain the invention as specified in claim 43.

i. *Referring to Claims 45, 59, and 64:*

As per Claim 45, Itkis discloses an information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure **[(Fig. 2)]**, said information processing device comprising:

to store a node key and a leaf key, the leaf key begin unique to the information processing device, and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure **[In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)]**; and

detect whether an encrypted version of the decryption key for decrypting encrypted data, and when the encrypted decryption key is detected, to calculate the decryption key by decrypting the encrypted decryption key **[performing no more than a predetermined number of decryption operations, the predetermined number being the same for all authorized devices, to obtain the content decryption key from an encrypted form thereof, the encrypted form being encrypted with a group key corresponding to a group of which the authorized device is a member (lines 54-59, Col. 3 from Itkis). A key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 670 are used, independently, to encrypt K (lines 43-46, Col. 9 from Itkis)]**, and

when the encrypted decryption key is not detected, to calculated the decryption key by decrypting a key block using at least one of the one or more node keys stored in the storage or the leaf key stored in the storage **[Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58,**

Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)].

Itkis discloses the hardware component for performing the encryption, decryption, and storage processes **[In a preferred embodiment of the present invention, an improved key distribution system is provided (lines 49-50, Col. 2 from Itkis). Each of the components of FIG. 1 is preferably implemented in a combination of software and computer hardware, as is well known in the art, and may include special purpose computer hardware, as is also well known in art, in order to increase efficiency of operation (lines 3-7, Col. 8 and Fig. 1). Individual components, described below, of the security**

element 120 may be implemented in hardware or in any suitable combination of hardware and software, as is well known in the art (lines 5-8, Col. 11 and Fig. 4)]. Itkis does not expressly disclose the hardware containing: (1) storage and encryption processor within the processing devices for holding the key information, calculate decryption key, and executing encryption/decryption processing, (2) the encrypted decrypting key is stored on the recording medium or in the recording area in the information processing device. However, Harada et al. disclose an LSI component, which contains the encryption and decryption units for deriving key information and performing encryption/decryption processes with keys and a storage unit for holding the relevant key information **[The disk key creation unit 1218 creates a 64-bit disk key including the information on the memory card ID that has been given from the memory card ID obtaining unit 1230. Here, a disk key is key data common to all kinds of memory card that is recording medium. The disk key encryption unit 1220 encrypts the disk key that has been created by the disk key creation unit 1218 using one of the plurality of master keys 1219 that have been stored in the disk key encryption unit 1220 in advance. The disk key encryption unit 1220 continues to encrypt the same disk key using a different master key 1219 to create the same**

number of encryption disk keys as that of the master keys 1219, and outputs the created encryption disk keys to the recording unit 1240 in the memory card writer 1200. The title key creation unit 1221 creates an appropriate 64-bit title key and gives the created title key to the title key encryption unit 1222. Here, the title key indicates key data that can be set for each music content (lines 8-24, Col. 13 from Harada et al.). Meanwhile, the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 29-34, Col. 13 and unit 1200 in Fig. 2 and 3 from Harada et al.)], and the encrypted decrypting key stored on a recording medium or in a storage area in said information processing device **[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-**

encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2 from Harada et al.)]. Dondeti et al. further disclose the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes **[Each member 22 is assigned a binary ID and these IDs are used to define key associations for each member 22 (lines 30-31, Col. 3). Members are represented by the leaves of a binary key distribution tree 26. Each member 22 generates a unique secret key 28 for itself and each internal node key is computed as a function of the secret keys of its two children. All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32 (lines 48-53, Col. 3). Internal nodes are associated with secret keys (lines 2-3, Col. 4)]** and Lotspiech et al. disclose use a generation number representing renewal information for a decryption key stored on at least one of the information processing device or the recording medium to **[a**

thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)]. Itkis, Harada et al., Dondeti et al., and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al. and Dondeti et al., and Lotspiech et al. since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of

encryption algorithms for distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.) and (2) to have a system for providing secure communication between many sends and many members (lines 15-17 from Dondeti et al.), and (3) to encrypt the broadcast programs such that an unauthorized clone receivers cannot easily decrypt the programs (lines 8-10, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis with Harada et al., Dondeti et al., and Lotspiech et al. to obtain the invention as specified in claim 45.

As per Claim 59, it is a method claim that encompasses limitations that are similar to those of the device Claim 45. Therefore, it is rejected with the same rationale applied against Claim 45 above.

As per Claims 64, it is a recording medium containing computer program claim corresponding to the method claim 59. Thus, it is rejected with the same rationale applied against Claim 59 above. In addition, Harada et al. disclose the computer program executed on an information processing device **[The personal computer 1100 is a personal computer that includes a CPU, a memory,**

a hard disk and the like and executes a program (lines 43-45, Col. 7 from Harada et al.)].

j. *Referring to Claims 46, 60, and 65:*

As per Claim 46, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 45, wherein, when the decryption key is not detected the decryption processor is further operable to encrypt the calculated decryption key and to store the encrypted decryption key on at least one of the recording medium or the memory **[(lines 12-15, 25-29, and 39-43, Col. 13 from Harada et al.)]**.

As per Claim 60, the rejection of Claim 59 is incorporated. In addition, Claim 60 encompasses limitations that are similar to those of Claim 46. Therefore, it is rejected with the same rationale applied against Claim 46 above. In addition, Itkis discloses said decrypting key calculated using at least one of the node key and the leaf key held in said storage means **[(lines 16-17 and 43-48, Col. 9 and Fig. 2 from Itkis)]**.

As per Claim 65, the rejection of Claim 64 is incorporated. In addition, Claim 65 is a recording medium claim corresponding to the method Claim 60. Therefore, it is rejected with the same rationale applied against Claim 60 above.

k. *Referring to Claims 47 and 61:*

As per Claim 47, Itkis, Harada et al., and Dondeti et al. disclose the information processing device as claimed in claim 45, wherein the decryption processor is further operable to decrypt the encrypted decryption key using at least one key unique to the information processing device when the encrypted decryption key is detected **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis)]**.

As per Claim 61, the rejection of Claim 59 is incorporated. In addition, Claim 61 encompasses limitations that are similar to those of Claim 47. Therefore, it is rejected with the same rationale applied against Claim 47 above.

l. *Referring to Claims 48 and 62:*

As per Claim 48, Itkis discloses an information processing method; comprising:

storing one or more node keys and a leaf key in an information processing device of one node of a hierarchical network of nodes having a hierarchical tree structure, each node key being unique to one node of the network, the leaf key being unique to the information processing device **[In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one**

of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)];

decrypting a key block using at least one of the stored node key and the stored leaf key **[Accompanying the content is a key block B (the key block can be assumed to include "media key" – e.g., the disc's serial number, etc. (lines 51-53, Col. 1 from Itkis). B can be computed (by the content providers, after examining the pirate devices) in such a way that all non-compromised devices can compute K from B (lines 56-58, Col. 1 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 and Fig. 2 from Itkis). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10 from Itkis). Thus, each device 110 need only perform one decryption operation in order to obtain K. It is**

appreciated that a further, typically fixed number of decryption operations, as is well known in the art, may need to be performed in order to actually obtain protected content (lines 12-16, Col. 10 from Itkis)];

calculating a decryption key usable to decrypt encrypted data stored on at least one of the information processing device or on a recording medium **[K may be typically be obtained from B in the present invention by a legitimate device in a single decryption operation (lines 58-60, Col. 2). Where K is a content encryption key or any other useful key (lines 7-8, Col. 10)]**; and

encrypting the decryption key using the key of the information processing device **[It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2. At any point, the keys of all groups 100 in the authorized set 60 are used, independently, to encrypt K (lines 41-46, Col. 9 from Itkis)]**.

Itkis does not expressly disclose storing the encrypted decryption key on at least one of the information processing device or on the recording medium and other limitations of the claim. However, Harada et al. disclose the encrypted decryption key, used for decrypting the content information, is stored on the recoding

medium and when it is determined that the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium **[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2)]**. Dondeti et al. further disclose the leaf key being unique to the information processing device such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network **[Each member 22 is assigned a binary ID and these IDs are used to define key**

associations for each member 22 (lines 30-31, Col. 3). Members are represented by the leaves of a binary key distribution tree 26. Each member 22 generates a unique secret key 28 for itself and each internal node key is computed as a function of the secret keys of its two children. All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32 (lines 48-53, Col. 3). Internal nodes are associated with secret keys (lines 2-3, Col. 4)], the key used in encrypting the calculated decrypting key is the leaf key **[Wherein, the first member uses the blinded keys received from the key association group and the first secret key to calculate an unblinded key of the first internal node (lines 48-51, Col. 2). All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32 (lines 52-53, Col. 3)]**, and using the leaf key to decrypt the encrypted decryption key to decrypt the encrypted data without having to decrypt the key block **[The root key is computed similarly and is used for data encryption. For each secret key, k, there is a blinded key, k', and an unblinded key. The blinded key is computed by applying a given one-way function to the secret key. Given a blinded key that is calculated with a one-way function, it is computationally infeasible to compute the unblinded**

counterpart of the blinded key. Each member 22 knows all the keys of the nodes in its path to the root of the tree and the blinded keys of siblings of the nodes in its path to the root of the tree and no other blinded or unblinded keys. The blinded keys are distributed by members that are owners and authorized distributors of those keys. Each member 22 computes the unblinded keys of the internal nodes of the tree in its path to the root and the root key itself, using the blinded keys it receives and its own secret key 28 (lines 4-19, Col. 4). All members in the multicast group can compute the root key with the given keys. A member with data to send, encrypts the data with the root key and sends it via traditional multicast channels (e.g.: MBONE). Other members can decrypt the data without any further key exchanges (lines 56-60, Col. 9)].

Lotspiech et al. disclose together with a generation number representing renewal information for the decryption key **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**; and

using the stored generation number to determine whether the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium **[a**

thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)].

Itkis, Harada et al., Dondeti et al., and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Itkis with Harada et al., Dondeti et al., and Lotspiech et al. since one would have been motivated to (1) provide a production protection system that enables contents to be recorded on a recording medium loaded on a player for replaying contents and the like in order to more intensively protect contents for sale, and enables one of encryption algorithms for

distributing contents via the Internet and for recording contents on the recording medium not to be influenced by the decryption of the other one (lines 53-60, Col. 1 from Harada et al.), (2) to have a system for providing secure communication between many sends and many members (lines 15-17 from Dondeti et al.), and (3) to encrypt the broadcast programs such that an unauthorized clone receivers cannot easily decrypt the programs (lines 8-10, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Itkis with Harada et al., Dondeti et al., and Lotspiech et al. to obtain the invention as specified in claim 48.

As per Claim 62, it is a recording medium containing computer program claim corresponding to the method claim 48. Thus, it is rejected with the same rationale applied against Claim 48 above. In addition, Harada et al. disclose the computer program executed on an information processing device **[The personal computer 1100 is a personal computer that includes a CPU, a memory, a hard disk and the like and executes a program (lines 43-45, Col. 7 from Harada et al.)]**.

m. <u>*Referring to Claim 51:*</u>

As per Claim 51, Itkis, Harada et al., Dondeti et al., and Lotspiech et al. disclose the information processing device as claimed in claim 48, wherein the encryption processor is operable to store

the decryption key encrypted using the leaf key unique to the information processing device **[(lines 54-59, Col. 3 and lines 43-48, Col. 9 from Itkis) and (lines 48-53, Col. 3; lines 2-3, Col. 4 from Dondeti et al.)]**. Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[(lines 21-23, Col. 6 from Lotspiech et al.)]**.

n. *Referring to Claims 57 and 63:*

As per Claim 57, it encompasses some limitations that are similar to those of Claim 48. Therefore, these limitations are rejected with the same rationale applied against Claim 48 above. In addition, Lotspiech et al. disclose the renewal generation number is associated with the number of the time the decryption key has been renewed **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]** and using the stored generation number to determine whether the decryption key is stored in the information processing device and when it is determined that the decryption key is stored in the information processing device **[a thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the**

message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)]. In addition, Harada et al. disclose using the decryption key to decrypt the encrypted data without having to decrypt the key block **[Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2). In a reverse order using the encrypted disk key and title key and to replay music by decrypting the audio data (lines 47-49, Col. 13)].**

As per Claim 63, it is a recording medium containing computer program claim corresponding to the method claim 57. Thus, it is

rejected with the same rationale applied against Claim 57 above. In addition, Harada et al. disclose the computer program executed on an information processing device **[The personal computer 1100 is a personal computer that includes a CPU, a memory, a hard disk and the like and executes a program (lines 43-45, Col. 7 from Harada et al.)]**.

o. *Referring to Claims 58:*

As per Claim 58, it encompasses some limitations that are similar to those of Claim 48. Therefore, these limitations are rejected with the same rationale applied against Claim 48 above. In addition, Harada et al. disclose storing the calculated decrypting key in the information processing device together with identification information, the identification information being usable to identify data decrypted using said decrypting key **[the memory card ID obtaining unit 1230 obtains the memory card ID that is inherent information from the memory card 1300, and gives the obtained memory card ID to the disk key creation unit 1218. When receiving the recording allowance, the recording unit 1240 records that data that have been output from the disk key encryption unit 1220, the title key encryption unit 1222, and the audio data encryption unit 1223 on the memory card 1300 (line 67, Col. 12 and lines 1-7, Col. 13 from Harada et al.). Meanwhile, the audio data encryption**

unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221 (lines 29-32, Col. 13 from Harada et al.)].

p. *Referring to Claim 68:*

As per Claim 68, Itkis, Harada et al., and Dondeti et al. disclose the recording medium as claimed in claim 62, wherein the method further comprises accessing the stored encrypted decryption key, recovering the decryption key be decrypting the encrypted decryption key using the leaf key, and decrypting content information stored on at least one of the recording medium or the storage using the recovered decryption key **[(lines 51-53 and 56-58, Col. 1; lines 12-16, Col. 10 from Itkis) and (lines 25-34 and 39-43, Col. 13; lines 37-48, Col. 16 from Harada et al.) and (lines 48-51, Col. 2 and lines 52-53, Col. 3 from Dondeti et al.)].**

q. *Referring to Claim 70:*

As per Claim 70, Itkis, Harada et al., and Dondeti et al. disclose the information processing apparatus as claimed in claim 34, wherein the encryption processor is further operable to access the stored encrypted decryption key, recover the decryption key by decrypting the encrypted decryption key using the leaf key, and decrypt content information stored on at least one of the recording

medium or the storage using the recovered decryption key **[(lines 51-53 and 56-58, Col. 1; lines 12-16, Col. 10 from Itkis) and (lines 25-34 and 39-43, Col. 13; lines 37-48, Col. 16 from Harada et al.) and (lines 48-51, Col. 2 and lines 52-53, Col. 3 from Dondeti et al.)]**.

r. *Referring to Claim 71:*

As per Claim 71, Itkis, Harada et al., and Dondeti et al. disclose the information processing apparatus as claimed in claim 70, wherein the decryption key includes a media key **[(lines 25-34 and 39-43, Col. 13 from Harada) and (lines 51-52, Col. 1 from Itkis)]**.

s. *Referring to Claim 72:*

As per Claim 72, Itkis, Harada et al., and Dondeti et al. disclose the information processing method as claimed in claim 48, further comprising accessing the stored encrypted decryption key, recover the decryption key by decrypting the encrypted decryption key using the leaf key, and decrypt content information stored on at least one of the recording medium or the storage using the recovered decryption key **[(lines 51-53 and 56-58, Col. 1; lines 12-16, Col. 10 from Itkis) and (lines 25-34 and 39-43, Col. 13; lines 37-48, Col. 16 from Harada et al.) and (lines 48-51, Col. 2 and lines 52-53, Col. 3 from Dondeti et al.)]**.

t. *Referring to Claim 73:*

As per Claim 73, Itkis, Harada et al., and Dondeti et al. disclose the information processing method as claimed in claim 72, wherein the decryption key includes a media key **[(lines 25-34 and 39-43, Col. 13 from Harada) and (lines 51-52, Col. 1 from Itkis)]**.

6. Claims 66-67 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harada et al. (U.S. Patent 6,687,683) in view of Itkis (U.S. Patent 6,880,081), Dondeti et al. (U.S. Patent 6,240,188), and Lotspiech et al. (U.S. Patent 6,118,873).

   a. *Referring to Claim 66:*

   As per Claim 66, Harada et al. disclose a recording medium having encrypted information recorded thereon including at least one of audio information, video information or human language text information in encrypted form **[The music content replay/recording system 1000 is a system in which a music content that has been received via a communication line 1001 is replayed using a personal computer 1100 and the music content is recorded on a memory card 1300 (lines 26-30, Col 7 from Harada et al.)]**, the encrypted information being decryptable only by any one of a plurality of information processing devices using a decryption key, the recording medium having the decryption key recorded thereon in encrypted form

[The title key encryption unit 1222 encrypts the title key that has been created by the title key creation unit 1221 using the disk that has been created by the disk key creation unit 1218, and outputs the encrypted title key to the recording unit 1240. Meanwhile the audio data encryption unit 1223 re-encrypts the C2 content 40 that has been output from the C2 content decryption unit 1217 using the title key that has been created by the title key creation unit 1221, and outputs the re-encrypted C2 content 40 to the recording unit 1240 (lines 25-34, Col. 13). Note that the recording unit 1240 records the audio data that has been transferred from the audio data encryption unit 1223 in an user accessible area in the memory card 1300 and the encrypted disk key and title key in a system area in the memory card 1300 that cannot be accessed by the user (lines 39-43, Col. 13 and Fig. 2 from Harada et al.). The encrypted C1 content 130 is data that is created by encrypting a plaintext, the C1 content 30 using the C1 key 21 (refer to FIG. 4), and the data length can change according to the content. The C1 key 21 is 40-bit key data, and the encryption using the C1 key 21 is performed in a block cipher system. For instance, a DES algorithm is used. The encrypted C2 content 140 is data that is created by encrypting a plaintext, the C2 content 40 using the C2 key 25

(refer to FIG. 4), and the data length can change according to the content. The C2 key 25 is 56-bit key data, and the encryption using the C2 key 25 is performed in a block cipher system. For instance, a DES algorithm is used (lines 37-48, Col. 16 from Harada et al.)]. Harada et al. do not expressly disclose the remaining limitation of the claim. However, Itkis and Dondeti et al. disclose the encrypted decryption key having been encrypted using a leaf key unique to one information processing device, the encrypted decryption key being stored as a key storage table together with identification for the one information processing device **[[In a preferable implementation of the group assignments 20 as shown in FIG. 1, the group assignments 20 may be depicted as a tree in which each one of the plurality of authorized devices is represented by a leaf (lines 21-26, Col. 8). At level n, the leaf level, each group 100 is associated with a device 110 (lines 16-17, Col. 9 from Itkis). It will be appreciated that the system of FIG. 1 is particularly useful as a solution of the key distribution problem in a case where a key is assigned to each of the groups 100 of FIG. 2 (lines 41-44, Col. 9 and Fig. 2 from Itkis)] and [Each member 22 is assigned a binary ID and these IDs are used to define key associations for each member 22 (lines 30-31, Col. 3). Members are represented by the leaves of a binary key**

distribution tree 26. Each member 22 generates a unique secret key 28 for itself and each internal node key is computed as a function of the secret keys of its two children. All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32 (lines 48-53, Col. 3). Internal nodes are associated with secret keys (lines 2-3, Col. 4)]], and Itkis further discloses a key storage table together with identification for the one information processing device **[1. Where K is a content encryption key or any other useful key, for example, device 110 can easily determine, based on group membership of the device 110 and, preferably, group identification accompanying each encryption of K in a key block B (lines 7-11, Col. 10 from Itkis)]**. Lotspiech et al. disclose the identification information being usable to determine whether the decryption key corresponding to the encrypted data is stored on the at least one of the information processing system or on the recording medium **[a thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the**

system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)], if so, the decryption key being usable to decrypt the encrypted data **[At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)]**. Harada et al., Itkis, Dondeti et al., and Lotspiech et al. are analogous art because they are from similar technology relating to the digital content information security and protection. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Harada et al. with Itkis and Dondeti et al. since one would have been motivated to (1) provide improved apparatus and methods for content access control and improved key distribution system (lines 47-50, Col. 2 from Itkis) and (2) to have a system for providing secure communication between many sends and many members (lines 15-17 from Dondeti et al.), and (3) to encrypt the broadcast programs such

that an unauthorized clone receivers cannot easily decrypt the programs (lines 8-10, Col. 1 from Lotspiech et al.). Therefore, it would have been obvious to combine Harada et al. with Itkis, Dondeti et al., and Lotspiech et al. to obtain the invention as specified in claim 66.

b. *Referring to Claim 67:*

As per Claim 67, Harada et al., Itkis, Dondeti et al., and Lotspiech et al. disclose the recording medium as claimed in claim 66, wherein the recording medium is removably insertable into any information processing device of the plurality of information processing devices through an opening in an exterior hosing of such information processing device, and is recordable to store the encrypted decryption key when the recording medium is inserted into the one information processing device **[(lines 25-34 and 39-43, Col. 13; lines 37-48, Col. 16; Fig. 1 and 2 from Harada et al.)]**.

c. *Referring to Claim 69:*

As per Claim 69, Harada et al., Itkis, Dondeti et al., and Lotspiech et al. disclose the recording medium as claimed in claim 67, wherein the decryption key includes a media key **[(lines 25-34 and 39-43, Col. 13 from Harada) and (lines 51-52, Col. 1 from Itkis)]**.

Allowable Subject Matter

7. Claims 36 and 50 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

8. Applicant's amendment, filed on Mar. 26, 2007, argues that none of the references cited teaches using a generation number as recited in Claim 34 to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key.
9. Applicant's remark has been fully considered, but found not persuasive based on the reasons below.

Regarding to Argument (1):

In regard to Applicant's argument that none of the references cited teaches using a generation number as recited in Claim 34 to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key, Examiner would like to point out the reference by Lotspiech et al.. In the reference by Lotspiech et al., it specifically discloses the generation number associated with the key, the generation number representing renewal information for the decryption key **[the renewal generation number refers to the number of times the keys of a device have been renewed (lines 21-23, Col. 6 from Lotspiech et al.)]**, and use

the generation number to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key **[a thirty two (32) bit renewal generation number field 50. Each device 18 determines whether the renewal generation number matches the renewal at which the particular device 18 is, and if so, the device 18 considers the message. Otherwise, the device 18 ignores the message. As described further below, in the presence of unauthorized devices the system 10 renews the device keys "S", and the renewal generation number refers to the number of times the keys of a device have been renewed (lines 15-23, Col. 6). At block 56, the device 18 decrypts a session key from the session key block for in turn decrypting the broadcast program. To do this, the device uses its device keys S_{ji}, i=1 to N, to decrypt the respective i^{th} session numbers x_i (lines 32-36, Col. 6)]**. Therefore, it is believed that the reference by Lotspiech et al. is sufficient to meet the argued limitation and the rejection to the independent claims with similar limitations are to be maintained.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

   a. Revital et al. (U.S. Pub. 20040101138) disclose a system and a method for secure distribution of digital media content through a packet-based network such as the Internet. The security of the

present invention does not require one-to-one key exchange, but rather enables keys, and/or information required in order to build the key, to be broadcast through the packet-based network. The digital media content is then also preferably broadcast, but cannot be accessed without the proper key. However, preferably only authorized end-user devices are able to access the digital media content, by receiving and/or being able to access the proper key. Thus, the present invention is useful for other types of networks in which digital media content is more easily broadcast rather than unicast, in addition to packet-based networks.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Jun. 08, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100